Form Approved
OMB No. 0704-0188

REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
21-10-16	Journal Article	01/2016 – 10/2016

4. TITLE AND SUBTITLE

Cyber Vigilance: The Human Factor

5a. CONTRACT NUMBER
FA8650-14-D-6501-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Ben D. Sawyer[1], Dr. Victor S. Finomore[2], Dr. Gregory J. Funke[3], Dr. Gerald Matthews[4], Dr. Vincent Mancuso[5], Dr. Matthew Funke[6], Dr. Joel S. Warm[3], and Dr. Peter A. Hancock[7]

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
H0JT (53291605)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

[1]Massachusetts Institute of Technology AgeLab, New England University Transportation Center, Cambridge, Massachusetts; [2]United States Air Force Academy, Colorado; [3]Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio; [4]Institute for Simulation and Training, University of Central Florida, Orlando, FL; [5]MIT Lincoln Laboratory, Lexington, MA; [6]Naval Medical Research Unit Dayton, Wright-Patterson Air Force Base, Ohio; [7]University of Central Florida, Orlando

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Materiel Command
Air Force Research Laboratory
711th Human Performance Wing
Airman Systems Directorate
Warfighter Interface Division
Applied Neuroscience Branch
Wright-Patterson Air Force Base, OH 45433

10. SPONSORING/MONITORING AGENCY ACRONYM(S)
711 HPW/RHCP/RHCPA

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
88ABW Cleared 12/03/2014; 88ABW-2014-5661; American Intelligence Journal

14.
Cyber-defenders face lengthy, repetitive work assignments with few critical signals and little control over what transpires. Their task is one of vigilance, well studied in contexts including air traffic control and medical monitoring. Cyber-defense display information density is several orders of magnitude above that seen in the aforementioned domains, and therefore blindly generalizing prior research is inadvisable. To understand this unique domain, we asked participants to perform a simulated cybersecurity task, searching for attack signatures in Internet traffic information. Consistent with results observed in "traditional" vigilance paradigms, signal detection declined significantly over time, it was directly related to signal probability, and it was inversely related to event rate. Reported high mental workload accompanied such degraded performance. These results highlight the necessity for understanding the physical and cognitive ergonomics underlying cyber-defense. They also suggest vulnerability to denial & deception (D&D) tactics which would effectively hack the human rather than the machine.

15. SUBJECT TERMS
Cyber, cyber defense, vigilance, event rate, signal probability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Gregory Funke
Unclassified	Unclassified	Unclassified	SAR	10	19b. TELEPHONE NUMBER

Cyber Vigilance:
The Human Factor

by Dr. Ben D. Sawyer, Dr. Victor S. Finomore, Dr. Gregory J. Funke, Dr. Gerald Matthews, Dr. Vincent Mancuso, Dr. Matthew Funke, Dr. Joel S. Warm, and Dr. Peter A. Hancock

OVERVIEW

Cyber-defenders face lengthy, repetitive work assignments with few critical signals and little control over what transpires. Their task is one of vigilance, well studied in contexts including air traffic control and medical monitoring. Cyber-defense display information density is several orders of magnitude above that seen in the aforementioned domains, and therefore blindly generalizing prior research is inadvisable. To understand this unique domain, we asked participants to perform a simulated cyber-security task, searching for attack signatures in Internet traffic information. Consistent with results observed in "traditional" vigilance paradigms, signal detection declined significantly over time, it was directly related to signal probability, and it was inversely related to event rate. Reported high mental workload accompanied such degraded performance. These results highlight the necessity for understanding the physical and cognitive ergonomics underlying cyber-defense. They also suggest vulnerability to denial & deception (D&D) tactics which would effectively hack the human rather than the machine.

INTRODUCTION

In a world of asymmetric conflict in which the dominant force of arms is owned by one side in the struggle, inherent conditions force the opposition to adopt new and innovative strategies and tactics if the warfare is to persist. Guerrilla tactics have always featured such necessary innovation, while the dominant entity similarly employs a variety of innovations to match evolving circumstances. Our age provides new opportunities; electronic networks such as the World Wide Web provide the opportunity to effect action at a distance. In many contemporary societies, predicated upon the foundation of safe, secure, and effective networks, disruption and destruction of hardware- and software-based systems pose crucial threats. Traditional D&D tactics take on new destructive and distractive power in a fully human-generated electronic environment. Unlike traditional conflict, attacks of this sort require no immediate physical presence of the attacker, and thus represent an appealing strategy to those constrained by kinetic force of arms.

In general, today there are cyber-attack forces which necessarily mandate the need for cyber-defense. As described by the previous Chief Scientist of the U.S. Air Force, Dr. Mark Maybury, cyberspace is a domain from and through which Air Force (AF) operations are performed, and it is essential for all such operations.[1] Of course, cyber-security extends well beyond military operations, but its centrality to national defense provides some idea of the importance of the domain. Given that importance, it is critical to maintain cyberspace security to prevent intrusion by foreign state actors, non-state actors (e.g., hackers), or even inadvertent interference.

The noisy, information-dense, human-conceived environment of cyber provides an excellent staging ground from which to practice the ancient art of deception.[2] A variety of strategies exists to deny access to real information about malicious network actions,[3] and although software initially identifies potential attacks such automation is never perfect. Thus, candidate attack events and false positives must be monitored by human observers who render the final decision. In small institutions, this process may be as simple as having an individual occasionally check for software alerts. However, within the present scale of military and civilian network activity, petabytes of data move between millions of addresses each day. As such, the human factor in military cyber-defense is larger by orders of magnitude. Dedicated teams of cyber-defenders are assigned to monitor algorithmically identified network traffic to determine if suspicious patterns warrant further detailed analysis. They then forward evidence to cyber forensic teams for subsequent examination.[4,5]

At present, contemporary cyber-intrusion detection systems are based solely on computer network analysis.[6] Though the algorithms and analytic techniques used in these systems vary considerably, most intrusion detection systems (IDS) identify malicious activity by algorithmically comparing current network activity to previously encountered or "known" malicious software signatures. This is also a key limitation of such systems—even slightly altering the underlying code of an attack may prevent its detection. To avoid this, IDS detection algorithms are purposely liberal, broadly flagging any activity that resembles a known

signature. Further complicating these issues are attacker attempts to disguise malicious code by creating deliberate similarities between attacks and "normal" traffic, which may greatly increase false positive rates. To supplement and improve IDS, cyber-defenders use a variety of tools, including hand-sorting, to discriminate attacks from false positives. This effort involves searching for specific patterns in information including key words and Internet protocol (IP) addresses, although the exact natures of the targets are changeable and unknown. Base rate of success is also unknown; while (in conventional warfare) casualties might be counted, a well-executed and successful cyber-attack may leave no trace.

In pursuing their mission, cyber-defenders face highly repetitive work assignments featuring large quantities of data (most of which are ultimately false positives) that must be processed. Embedded in these trains of information are few critical occurrences. Cyber-defenders have little control over the rate at which such critical events appear and, as candidate signals are passed on to other teams, have little knowledge of their ultimate resolution. Their task bears the hallmark of what is known in the ergonomics and human factors community as a *vigilance task,* in which operators must focus their attention and detect infrequently occurring critical signals over prolonged periods of time.[7 8] Understanding of vigilance tasks and appropriate countermeasures are crucial in many working environments wherein such semi-automated systems are featured. Some of these include air traffic control, cockpit display monitoring, airport security, industrial process control, long distance driving, and the monitoring of anaesthesia gauges during surgery, among many others. Accidents ranging from minor to major have resulted from vigilance failures by human observers.[9] Consequently, one can posit that cyber-security operations could take advantage of what is known about vigilance in order to enhance their mission success rate. However, this presently appears to be an unexplored opportunity.

To date, the only study to examine vigilance performance in cyberspace was carried out by McIntire and her associates.[10] They showed that the vigilance decrement, the temporal decline in signal detection that typifies vigilance performance,[11 12], also occurred in a simulated cyber task, and that the decrement was accompanied by changes in oculomotor activity, such as blink frequency and duration, and pupil diameter, which they argued could be employed to detect when cyber operators are in need of rest or replacement.

In addition to time on task, vigilance performance is determined by a number of psycho-physical factors which confront observers with perceptual challenges. Knowledge of those challenges could enable designers to develop cyber displays that can be interrogated more effectively by observers.[13 14] Accordingly, one goal for our present study was to extend the link between vigilance and cyber tasks by determining if two of the most critical psycho-physical factors, signal probability and event rate, would affect performance on a simulated cyber task. Signal probability refers to the likelihood that any stimulus event is a critical signal, while event rate refers to the number of stimulus events that must be monitored in order to detect critical signals.

...attacks in the field, especially those of real consequence, are so diluted in the high event rate as to qualify as the putative "black swans."

Performance efficiency in vigilance tasks varies directly with the probability of critical signals and inversely with event rate.[15 16] Event rate might defensibly be labelled "self-paced" in many real-world cyber-defense environments. However, overall event rate is a function of the total candidate signals over time, divided of course by the workforce size available. This is a metric that readily indexes to the macro view of cyber-defense: rapid growth in infrastructure coupled with a shortage of information security professionals. Our current task presented stimuli at a controlled rate. Given the supposition that actual events in the field are high and climbing we have chosen to explore precisely what, in the context of information processing demands, is a demanding event rate. Conversely, signal probability in cyber-defense, although not known, is likely well below the 5% "low" rate of our present experiment. This probability is a practicality of experimental design since we must have enough candidate signals to observe variation between groups. It is worth noting, however, that attacks in the field, especially those of real consequence, are so diluted in the high event rate as to qualify as the putative "black swans."[17]

In addition to confronting observers with perceptual challenges, vigilance tasks also induce high levels of perceived mental workload[18] as reflected by the NASA-Task Load Index,[19] which is considered to be one of the most effective measures of perceived mental workload currently available.[20] It provides a measure of overall or global workload on a 0-100 scale and identifies the relative contribution of six sources of workload: Mental Demand, Physical Demand, Temporal Demand, Performance, Effort, and Frustration. As summarized by Finomore, Shaw, Warm, Matthews, and Boles,[21] Warm et al.,[22] and Wickens

et al.,[23] a number of studies have shown that the global workload scores on vigilance tasks fall at the upper end of the NASA-TLX scale and that Mental Demand and Frustration are the primary drivers of such high workload levels in vigilance tasks. A second goal for the present study was to determine if a simulated cyber task would also induce hard work in observers, and if Mental Demand and Frustration would be the primary components of that workload in the cyber task that we employed. Such knowledge may help supervisors and designers better understand observers' reactions to cyber monitoring assignments.

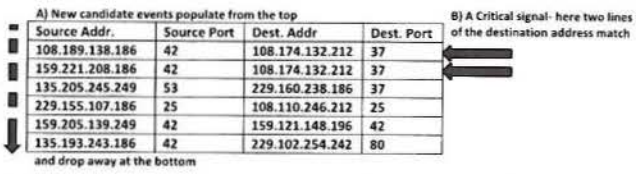
METHODOLOGY

Participants

The study was conducted at the Air Force Research Laboratory (AFRL), Wright-Patterson Air Force Base (WPAFB). Twenty-four volunteers (14 men and 10 women) were recruited from base personnel and the local population and paid a total of $45 each for their participation. All participants had 20/20 or corrected vision and no history of neurological problems. The study was approved by the WPAFB Institutional Review Board (IRB).

Apparatus and Procedure

Participants assumed the role of a cyber-defender monitoring strings of IP addresses and communication port numbers on a computer display. The task, which was similar to that employed by McIntire et al.,[24] was developed by the University of Dayton Research Institute (UDRI) to simulate a task that was representative of cyber-defense operations. As shown in Figure 1, the waterfall display was composed of two columns of six IP addresses, each containing 12 digits, and two columns of six communication port numbers, each containing two digits. The task of the cyber-defender was to look for cases in which the IP address and associated communication port number at the top position of any column completely matched an IP address/communication port number that was already present in any one of the other positions in *that* column (the critical signal for detection). At regular intervals throughout the task, the display would refresh and two new IP address/ communication port numbers would appear in the top position of the columns. The previous entries would then move down to the next row immediately below the top position and the bottom series would disappear from the display.



Source Addr.	Source Port	Dest. Addr	Dest. Port
108.189.138.186	42	108.174.132.212	37
159.221.208.186	42	108.174.132.212	37
135.205.245.249	53	229.160.238.186	37
229.155.107.186	25	108.110.246.212	25
159.205.139.249	42	159.121.148.196	42
135.193.243.186	42	229.102.254.242	80

Figure 1. Above, a screenshot of the waterfall display used in the cyber task. A critical signal is present in the rightmost "Dest. Port" column, as there is a match between the IP address and associated communication port of the top position and the second position. In 3.75 or 7.5 seconds, dependent on event rate, another line of IP addresses would drop down from the top, and the bottom line would drop away.

We acknowledge here that the critical signal for detection employed in *this* experiment could be algorithmically identified and the associated attack automatically prevented by an intrusion detection system due to its relative unsophistication. However, in "real-world" cyber defense contexts novel signatures are encountered for which there is not an existing algorithmic response. In such instances, human operators must detect and respond to attacks exploiting that vulnerability while the algorithmic defense is coded and put into place. We intended the context of the current experiment to represent just such an occurrence. More broadly, many present cyber-displays present far more information in far less time than any "classical" vigilance experiment display, and thus the present experiment can build understanding of whether vigilance decrements might be seen in such informationally dense tasks.

Two levels of signal probability (low vs. high) were combined with two levels of event rate (slow vs. fast) to produce four experimental conditions. Six participants were assigned at random to each of these four conditions. All participants completed a 40- minute vigil divided into four continuous 10-minute periods of watch. During the task, strings of IP addresses and port numbers were always visible on the computer screen. In the slow event rate-high signal probability condition, the display was updated eight times/min with a 20% chance of the appearance of a critical signal. In the slow event rate-low signal probability condition, updates also occurred eight times/min but with a 5% chance of critical signal appearance. In the fast event rate-high signal probability condition, the display was updated 16 times/min with a 20% chance of the presence of a critical signal. In the fast event rate-low signal probability condition, updates also occurred 16 times/min but with a 5% chance of critical signal appearance. Critical signal appearance was scheduled so that only one of the two IP address/communication port columns would have a signal at any given time. Participants responded to critical signals by pressing the spacebar on the computer keyboard.

Responses occurring within three seconds of the appearance of a critical signal were considered correct detections. All other responses were scored as false alarms. The participants were aware of this scoring procedure.

Preceding the 40-minute vigil, participants were given a 15-minute training period on the cyber task. During that training period the program played recorded auditory feedback in the form of a male voice, indicating correct detections, misses, and false alarms. Feedback was not provided during the main task itself. Immediately following the conclusion of that task, participants completed a computerized version of the NASA-TLX.

RESULTS

Performance Efficiency

Mean percentages of correct detections and their associated standard errors for all combinations of event rate, signal probability, and time on task are presented in Table 1.

Table 1. Mean percent correct detection scores for all combinations of signal probability and event rate during each period of watch.

		Period of Watch (10 minutes)				
Signal Probability	Event Rate	1	2	3	4	Mean
Low	Slow	**87.50**	**95.83**	**95.83**	**75.00**	**88.54**
		(5.59)	(4.17)	(4.17)	(15.81)	(7.43)
	Fast	**60.42**	**60.42**	**58.33**	**43.75**	**55.73**
		(7.51)	(7.51)	(6.97)	(7.74)	(7.43)
High	Slow	**95.83**	**91.67**	**88.54**	**80.21**	**89.06**
		(1.32)	(3.84)	(2.98)	(6.13)	(3.57)
	Fast	**77.08**	**77.60**	**76.56**	**77.60**	**77.21**
		(5.33)	(6.01)	(7.38)	(4.80)	(5.88)
Mean		**80.21**	**81.38**	**79.82**	**69.14**	
		(4.94)	(5.38)	(5.38)	(8.62)	

Note: Standard errors are in parentheses.

Perusal of Table 1 reveals that detection rates were lower in the case of the low ($M = 72.14\%$) signal probability condition as compared to the high ($M = 83.14\%$). Mean detection scores were higher in the slow ($M = 88.80\%$) event rate condition as compared to the fast ($M = 66.47\%$). In addition there was a notable decline in signal detections during the final period of watch. These patterns were confirmed by a 2 (event rate) × 2 (signal probability) × 4 (periods of watch) mixed-model analysis of variance (ANOVA) of the arcsines of the percentage of correct detections. This analysis indicated statistically significant main effects for signal probability, $F(1, 20) = 4.26, p = .05, \eta_p^2 = .18$ event rate, $F(1, 20) = 17.53, p < .001, \eta_p^2 = .47$, and period of watch, $F(2.05, 40.93) = 5.44, p = .008, \eta_p^2 = .21$. The remaining sources of variance in the analysis were not significant ($p > .05$ in each case). However, the Signal Probability by Event Rate interaction closely approached the traditional level of significance, $F(1,20) = 3.86, p = .06, \eta_p^2 = .16$. In this, as well as in the analysis of the workload scores which follow, the Box correction was applied when appropriate to compensate for violations of the sphericity assumption.[25]

The Signal Probability by Event Rate interaction is illustrated in Figure 2. It is evident in the graphic that the scores for the two signal probability conditions were similarly high in the context of the slow event rate. By contrast, in the context of a fast event rate, performance efficiency in the high probability condition was considerably better than in the low probability condition.

False alarms were rare in this study. The overall false alarm percentage across all experimental conditions was < 1%. Consequently, false alarms were not analyzed further.

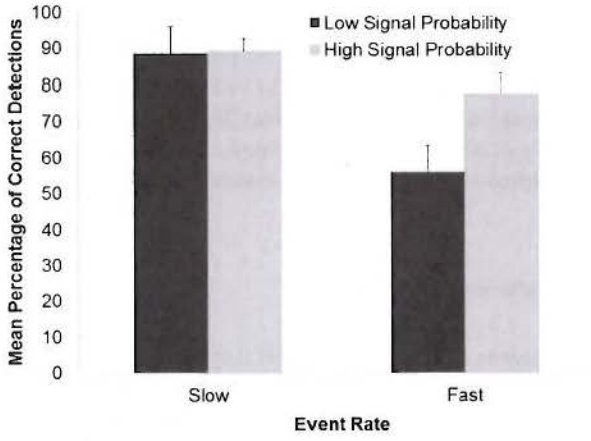


Figure 2. Mean percent detection scores for all combinations of signal probability and event rate. Error bars are standard errors.

Subjective Workload

Observers in all task conditions rated their workload on the six subscales of the NASA-TLX. Following a procedure recommended by Nygren,[26] workload scores were based solely on the ratings themselves and not on associated weightings for each subscale. Mean workload values for all combinations of event rate, signal probability, and NASA-TLX subscales are presented in Table 2.

Table 2. Mean NASA-TLX subscale scores for all combinations of signal probability and event rate.

		Subscale						
Signal Probability	Event Rate	MD	PD	TD	P	E	F	Composite
Low	Slow	72.50	15.00	75.00	33.33	72.50	39.17	51.25
		(11.38)	(4.65)	(6.45)	(13.08)	(6.55)	(14.34)	(9.41)
	Fast	67.50	33.33	77.50	42.50	80.00	50.83	58.61
		(10.63)	(9.55)	(8.14)	(9.73)	(9.31)	(11.36)	(9.78)
High	Slow	85.83	4.17	55.00	23.33	62.50	33.33	44.03
		(3.75)	(0.83)	(13.66)	(5.87)	(12.23)	(10.46)	(7.80)
	Fast	86.67	17.50	82.50	45.00	80.00	51.67	60.56
		(5.11)	(8.73)	(7.39)	(12.32)	(7.64)	(8.82)	(8.33)
Mean		78.13	17.50	72.50	36.04	73.75	43.75	53.61
		(7.72)	(5.94)	(8.91)	(10.25)	(8.93)	(11.25)	(8.83)

Note: Standard errors are in parentheses. Mean NASA Task Load Index (TLX) scores are listed for the subscales of Mental Demand (MD), Physical Demand (PD), Temporal Demand (TD), Performance (P), Effort (E), and Frustration (F).

As can be seen in Table 2, the overall composite workload rating for all task conditions ($M = 53.61$) fell above the midpoint of the scale (50), suggesting that participants found the cyber monitoring assignment to be demanding. A 2 (event rate) × 2 (signal probability) × 6 (subscales) mixed ANOVA of the workload data revealed a significant main effect for event rate, $F(1, 20) = 5.32, p = .03, \eta_p^2 = .21$, signifying that observers in the fast event rate condition ($M = 59.58$) found their vigilance assignments to be more challenging than those in the slow event rate condition ($M = 47.64$). A significant main effect was also found for subscales, $F(2.88, 57.66) = 33.02, p < .001, \eta_p^2 = .62$. Bonferroni-corrected t-tests with alpha set at .05 indicated that participants perceived Mental Demand, Temporal Demand, and Effort as the greatest contributors to overall workload in the present circumstances. The means for these scales, which fell at the upper level of the workload index, differed significantly from those of all the other scales ($p < .05$ in all cases) but not from each other. The main effect for signal probability and all of the interactions in the analysis lacked significance ($p > .05$ in all cases).

DISCUSSION

Consistent with results first reported by McIntire et al.,[27] performance efficiency on the cyber task was susceptible to the vigilance decrement. In the present case, the decrement consisted of a notable drop in signal detection during the last period of watch after participants had maintained a stable level of performance across three earlier watchkeeping periods. The temporal step-function in regard to the cyber task differs from the decrement seen in more traditional vigilance tasks in which typically there is a negatively accelerated progressive decline in performance efficiency over time.[28] A major theory used to account for the deterioration of performance efficiency over time characteristic of vigilance tasks is anchored in resource theory, wherein a limited-capacity information processing system allocates resources or reservoirs of energy to deal with the tasks that confront it. Since vigilance tasks require observers to make continuous signal/noise discriminations without rest, such tasks deplete available cognitive resources over time, which results in the vigilance decrement.[29 30 31 32] The step-function observed in our present study may be based on a combination of both motivation and resource loss.[33 34] More specifically, since the present participants were engaged in what they were informed was a critical Air Force assignment—cyber-defense—and were paid a substantial sum for serving in the study, they may have been motivated to sustain a high level of performance. However, over time they were unable to do so, potentially because of diminished information processing resources, a situation that is arguably reflected in the high scores seen on the NASA TLX, especially in the Effort subscale.

It is evident that operators cannot sustain performance in cyber tasks such as the one presented by our testbed over prolonged intervals of time. Consequently, this finding must be considered in work scheduling.

We should note that it was not a forgone conclusion that the information-rich cyber task would result in any form of decrement. Some complex tasks exhibit attenuated or absent decrements, especially when they involve diverse subtasks.[35 36] In other cases however, complexity can amplify the decrement.[37 38] Given the pattern we observed, cyber tasks appear to fall in the former category.

It is evident that operators cannot sustain performance in cyber tasks such as the one presented by our testbed over prolonged intervals of time. Consequently, this finding must be considered in work scheduling. Given the present data, instituting a 30-minute shift length for operators should be beneficial. Further, as McIntire and her associates have indicated,[39] the development of non-invasive methods could enable supervisors to monitor a cybersecurity operator's need for rest or replacement. The oculomotor changes described by McIntire et al.,[40] such as increased blink rate and longer blink durations, offer one approach by which supervisors might "monitor the monitor."

Another possibility that supervisors of cyber-security operators might consider is the use of Transcranial Doppler (TCD) sonography, a non-invasive neuroimaging method involving sensors worn in a headband, to assess cerebral blood flow velocity (CBFV). Several studies have

shown that the vigilance decrement is accompanied by a decline in CBFV, and that the changes in CBFV can forecast declines in operator efficiency.[41 42 43 44] Regarding electroencephalography (EEG), increases in lower frequency alpha power (8-10.9 Hz) also appear to be diagnostic of loss of vigilance in high event rate tasks.[45]

Consistent with the findings of a large number of vigilance studies,[46 47] participants in the cyber task benefited from a high level of signal probability. In an insightful analysis of human factors principles involved in the control of vigilance, Craig pointed out that one way to enhance the quality of sustained attention in operational settings is to reduce signal uncertainty.[48] Increments in signal probability clearly reduce signal uncertainty. Consequently, when signal probability is low, as is often the case in cyber-security operations, controllers might give some thought to introducing artificial signals in order to increase signal probability and thereby the likelihood of critical signal detection. A strategy of that sort would require careful thought, however, for as Craig (1984) has pointed out, artificial signals also increase the frequency of false alarms, which themselves can have a negative impact on cyber-security operations.[49]

Clearly, event rate is a key factor in cyber performance and should be considered in the design of cyber-security systems.

The concept of boosting detection through artificial inflation of signal probability gives rise to a corollary potential: a prevalence denial attack (PDA) upon enemy operators. By flooding a network with "grey signals," purposely built to be flagged by algorithmic defense systems but easily identified as non-threats by human operators, an aggressor would artificially depress the signal probability of candidate events presented to cyber-defenders. This imposition of impoverished signal probability would compromise operator accuracy, allowing genuine attacks a greater chance to avoid human detection. Such a "PDA," therefore, represent a style of D&D perhaps analogous to the Chinese concept of "seduction," in which an enemy is induced to make a fatal mistake.[50]

Vigilance experiments often employ dynamic displays wherein the critical signals for detection are embedded in a matrix of recurring neutral background events. Although the background events may be neutral in the sense that they require no overt response from the observer, they are far from neutral in their influence on signal detection.[51] Signal detections vary inversely with event rate, and event rate serves as a moderator variable for other psychophysical factors. For example, the degrading effects of low signal probability are magnified in the context of a fast as compared to a slow event rate.[52 53] Outcomes such as these were evident in the cyber task that we employed in this study. Signal detection was poorer in the context of a fast as compared to a slow event rate and the differential effects of variations in signal probability were observed only in the fast event rate condition.

Clearly, event rate is a key factor in cyber performance and should be considered in the design of cyber-security systems. As with the case of the vigilance decrement, the effects of event rate can also be accounted for on the basis of the resource model. Fast event rates require observers to make more frequent signal/noise discriminations than slow event rates and, therefore, deplete information-processing assets to a greater degree.[54] From an operational viewpoint, it might seem reasonable to expect that the more an operator is required to view the cyber display, the more likely the operator is to detect adverse events. The event rate effect indicates this is not necessarily so, and designers of cyber displays should be heedful of establishing an event rate that maximizes performance in the systems that they develop.

Along this line, we should note that, in traditional vigilance tasks, event rates which are below 24 events/min are categorized as slow, while those greater than 24 events/min are considered as fast[55 56]. In our current study, 8 events/min constituted the slow event rate while the fast event rate was only 16 event/min, a value well below the 24 event/min criterion for the definition of a fast event rate. The fast event used in the present experiment was chosen because pilot work revealed that observers could not perform the task effectively at event rates of 24/min or more. Evidently, cyber task performance is extremely sensitive to event rate effects.

At first glance, vigilance tasks can seem to be relatively simple and under-stimulating assignments since all observers are required to do is view a display and take action when a critical event occurs. On the contrary, Hancock and Warm[57] were the first to propose, and then subsequently demonstrate that that the cost of mental operations in vigilance is high.[58] This proposition has been confirmed a number of times, as reflected in scores on the NASA-TLX and the finding that Mental Demand and Frustration are the primary components of workload in vigilance.[59 60 61] Our present results indicate that cyber operations also induce high levels of mental demand as seen through the lens of the NASA-TLX—overall workload ratings were above the midpoint of the NASA-TLX and the scores for the Mental Demand, Temporal Demand, and Effort components of workload fell at the upper level of the workload index.

It is of interest to note that, while the portrait of critical workload components in the present cyber task included

Mental Demand, it also included Temporal Demand and Effort, which are not often included in the ensemble of key workload elements identified in more traditional vigilance tasks. These differences in the profile of workload components may be related to the need for rapid responding and display scanning inherent in the cyber task employed herein and to the participants' awareness of the importance of the task they were performing for Air Force operations.

As described by Wickens et al.,[62] mental workload characterizes the demands that tasks make on the limited information processing capacity of observers. Excessive levels of demand lead to declines in performance efficiency and to heightened levels of task-related stress.[63] Consequently, the high level of workload reported in the current experiment should be a concern to designers of cybersecurity interfaces. From the resource view, care should be taken not to develop cyber displays in which mental demands exceed resource supply, and to generate remedies for cyber tasks that pose threats to that supply. Given the high workload of cyber tasks, managers should be mindful of the fact that cyber tasks can be stressful and of the implications of stress for performance efficiency and operator health.[64] [65]

In sum, our study was conducted to determine if cyber tasks are linked to more traditional vigilance tasks. The answer to that question is a resounding "yes." Accordingly, cyber system designers need to be aware of the information-processing demands imposed by vigilance tasks and the steps that can be taken to minimize the negative effects of these demands on operator performance in cyber environments. We identify two classic factors on which—in cyber tasks as in "classical" vigilance—such vigilance performances hinges: event rate and signal probability. The former is firmly in the hands of the defender, as the number of operators may be ramped up to satisfy demand, and as such can be considered in part a human resources problem. The latter, signal probability, is more problematic. Although artificial "critical events" might be introduced to boost operator performance, such tactics have drawbacks. An attacker, however, would have little difficulty boosting "non-critical events," to the detriment of cyber-defender performance, in a D&D PDA (prevalence denial attack). Immediate action can be taken to reduce the above identified risks, and they also reveal as critical the ongoing push to train more cyber-defenders. Such steps are vitally necessary to address not only algorithmic challenges in cyber-defense but also the human factor.

Notes

[1] Mark T. Maybury, "Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision, 2012-2025" (Washington, DC: U.S. Air Force Chief Scientist, December 13, 2012).

[2] Peter A. Hancock, *Hoax Springs Eternal: The Psychology of Deception* (New York: Cambridge University Press, 2015).

[3] Neil C. Rowe, "A Taxonomy of Deception in Cyberspace," International Conference on Information Warfare and Security, Princess Anne, MD, March 2006, 173-181.

[4] Anita D'Amico et al., "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts," proceedings of *The Human Factors and Ergonomics Society Annual Meeting* 49 (2005): 229-233.

[5] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010): 63-86.

[6] Shailendra Singh and Sanjay Silakari, "A Survey of Cyber Attack Detection Systems," *International Journal of Computer Science and Network Security* 9 (2009): 1-10.

[7] Peter A. Hancock, "In Search of Vigilance: The Problem of Iatrogenically Created Psychological Phenomena," *American Psychologist* 68 (2013): 97-109.

[8] Joel S. Warm, Raja Parasuraman, and Gerald Matthews, "Vigilance Requires Hard Mental Work and Is Stressful," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 50 (2008): 433-441.

[9] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.

[10] Lindsey McIntire et al., "Eye Metrics: An Alternative Vigilance Detector for Military Operators," *Military Psychology* 25, no. 5 (2013): 502.

[11] David Roy Davies and Raja Parasuraman, *The Psychology of Vigilance* (London: Academic Press, 1982).

[12] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.

[13] Peter A. Hancock, "In Search of Vigilance: The Problem of Iatrogenically Created Psychological Phenomena," *American Psychologist* 68 (2013): 97-109.

[14] Peter A. Hancock, "Finding Vigilance through Complex Explanations for Complex Phenomena," *The American Psychologist* 69 (2014): 86-88.

[15] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.

[16] Joel S. Warm and Harry J. Jerison," The Psychophysics of Vigilance," in *Sustained Attention in Human Performance*, ed. Joel S. Warm (Chichester, UK: Wiley, 1984), 15-59.

[17] Nassim Nicholas Taleb, "Black Swans and the Domains of Statistics," *The American Statistician* 61, no. 3 (2007): 198-200.

[18] Peter A. Hancock and Joel S. Warm, "A Dynamic Model of Stress and Sustained Attention," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 31, no. 5 (1989): 519-537.

[19] Sandra G. Hart and Lowell E. Staveland, "Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research," *Advances in Psychology* 52 (1988): 139-183.

[20] Christopher D. Wickens, *Engineering Psychology and Human Performance*, 4th ed. (Boston: Pearson, 2013).

[21] Victor S. Finomore et al., "Viewing the Workload of Vigilance through the Lenses of the NASA-TLX and the MRQ," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 55, no. 6 (2013): 1044-1063.

[22] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[23] Christopher D. Wickens, *Engineering Psychology and Human Performance*, 4th ed. (Boston: Pearson, 2013).
[24] Lindsey McIntire et al., "Eye Metrics: An Alternative Vigilance Detector for Military Operators," *Military Psychology* 25, no. 5 (2013): 502.
[25] Andy Field, *Discovering Statistics Using SPSS* (Sage Publications, 2009).
[26] Thomas E. Nygren, "Psychometric Properties of Subjective Workload Measurement Techniques: Implications for Their Use in the Assessment of Perceived Mental Workload," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 33 (1991): 17-33.
[27] Lindsey McIntire et al., "Eye Metrics: An Alternative Vigilance Detector for Military Operators," *Military Psychology* 25, no. 5 (2013): 502.
[28] David Roy Davies and Raja Parasuraman, *The Psychology of Vigilance* (London: Academic Press, 1982).
[29] Ibid.
[30] Peter A. Hancock and Joel S. Warm, "A Dynamic Model of Stress and Sustained Attention," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 31, no. 5 (1989): 519-537.
[31] Robert W. Proctor and Kim-Phuiong Vu, "Cumulative Knowledge and Progress in Human Factors," *Annual Review of Psychology* 61 (2010): 623-651.
[32] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, ed. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[33] James L. Szalma, "On the Application of Motivation Theory to Human Factors/Ergonomics Motivational Design Principles for Human-Technology Interaction," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 56 (2014): 1453-1471.
[34] Tarah N. Schmidt et al., "The Effect of Video Game Play on Performance in a Vigilance Task," proceedings of *the Human Factors and Ergonomics Society* 56 (2012): 1544-1547.
[35] Jack A. Adams and John M. Humes, "Monitoring of Complex Visual Displays: Training for Vigilance," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 5 (1963): 147-153.
[36] Thomas Lanzetta, "Effects of Task Type and Stimulus Homogeneity on the Event Rate Function in Sustained Attention," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 29 (1984): 625-633.
[37] Joel S. Warm and Harry J. Jerison," The Psychophysics of Vigilance," in *Sustained Attention in Human Performance*, ed. Joel S. Warm (Chichester, UK: Wiley, 1984), 15-59.
[38] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[39] Lindsey McIntire et al., "Eye Metrics: An Alternative Vigilance Detector for Military Operators," *Military Psychology* 25, no. 5 (2013): 502.
[40] Ibid.
[41] Gerald Matthews et al., "Task Engagement, Cerebral Blood Flow Velocity, and Diagnostic Monitoring for Sustained Attention," *Journal of Experimental Psychology: Applied* 16 (2010): 187-203.
[42] Lauren Elizabeth Reinerman-Jones et al., "Selection for Vigilance Assignments: A Review and Proposed New Direction," *Theoretical Issues in Ergonomic Science* 12, no. 4 (2011): 273-296.
[43] Tyler H. Shaw et al., "Event-Related Cerebral Hemodynamics Reveal Target-Specific Resource Allocation for Both 'Go' and 'No-Go' Response-Based Vigilance Tasks," *Brain and Cognition 82*, no. 3 (2013): 265-273.
[44] Joel S. Warm, Gerald Matthews, and Raja Parasuraman, "Cerebral Hemodynamics and Vigilance Performance," *Military Psychology* 21, no. S1 (2009): S75-S100.
[45] Altyngul T. Kamzanova, Almira M. Kustubayeva, and Gerald Matthews, "Use of EEG Workload Indices for Diagnostic Monitoring of Vigilance Decrement," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 56, no. 6 (2014): 1136-1149.
[46] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[47] Joel S. Warm and Harry J. Jerison," The Psychophysics of Vigilance," in *Sustained Attention in Human Performance*, ed. Joel S. Warm (Chichester, UK: Wiley, 1984), 15-59.
[48] Angus Craig, "Human Engineering: The Control of Vigilance," in *Sustained Attention in Human Performance*, ed. Joel S. Warm (New York: Wiley, 1984), 247-291.
[49] Ibid.
[50] Michael Pillsbury, "China's Military Strategy toward the US: A View from Open Sources," November 2001: 4.
[51] Peter A. Hancock, "In Search of Vigilance: The Problem of Iatrogenically Created Psychological Phenomena," *American Psychologist* 68 (2013): 97-109.
[52] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[53] Joel S. Warm and Harry J. Jerison, "The Psychophysics of Vigilance," in *Sustained Attention in Human Performance*, ed. Joel S. Warm (Chichester, UK: Wiley, 1984), 15-590.
[54] David Roy Davies and Raja Parasuraman, *The Psychology of Vigilance* (London: Academic Press, 1982).
[55] Ibid.
[56] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[57] Peter A. Hancock and Joel S. Warm, "A Dynamic Model of Stress and Sustained Attention," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 31, no. 5 (1989): 519-537.
[58] Joel S. Warm, William N. Dember, and Peter A. Hancock, "Vigilance and Workload in Automated Systems," in *Automation and Human Performance: Theory and Applications*, eds. Raja Parasuraman and Mustapha Mouloua (Mahwah, NJ: Erlbaum, 1996), 183-200.
[59] Victor S. Finomore et al., "Viewing the Workload of Vigilance through the Lenses of the NASA-TLX and the MRQ," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 55, no. 6 (2013): 1044-1063.
[60] Joel S. Warm et al., "Vigilance: A Perceptual Challenge," in *Handbook of Applied Perception*, eds. Robert R. Hoffman et al. (New York: Cambridge University Press, forthcoming), 241-283.
[61] Christopher D. Wickens, *Engineering Psychology and Human Performance*, 4th ed. (Boston: Pearson, 2013).
[62] Ibid.

[63] Tarah N.Schmidt et al., "The Effect of Video Game Play on Performance in a Vigilance Task," proceedings of *the Human Factors and Ergonomics Society Annual Meeting* 56, no. 1 (2012): 1544-1547.
[64] Peter A. Hancock and Joel S. Warm, "A Dynamic Model of Stress and Sustained Attention," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 31, no. 5 (1989): 519-537.
[65] Raymond S. Nickerson, *Looking Ahead: Human Factors Challenges in a Changing World* (Mahwah, NJ: Erlbaum, 1993).

Dr. Ben D. Sawyer is a Postdoctoral Associate at MIT AgeLab and a Research Associate at the University of Central Florida's MIT^2 Laboratory. Dr. Sawyer received his PhD in Applied Experimental Psychology and Human Factors from UCF in 2015, and additionally holds an MS in Industrial Engineering. His research interests center around successes and failure of human attention, especially in high workload environments. He is a past Repperger Scholar with the U.S. Air Force Research Laboratory's 711th Human Performance Wing, where he performed the work described here as a member of the Applied Neuroscience Division.

Dr. Victor S. Finomore is an Engineering Research Psychologist at the Air Force Research Laboratory, 711th Human Performance Wing, Warfighter Interface Division, currently serving as Distinguished Visiting Research Fellow at the U.S. Air Force Academy and Technical Advisor to the Warfighter Effectiveness Research Center. He received his PhD in Experimental Psychology from the University of Cincinnati in 2008. His research interests include multimodal displays, cognitive workload, decision-making, and human performance. His research supports Air Force Special Operations' battlefield airmen, command and control, and cyber operators.

Dr. Gregory J. Funke is the leader of the Team Performance and Basic Cyber Research group of the Cognitive Performance Optimization Section in the Air Force Research Laboratory's Applied Neuroscience Branch, Warfighter Interface Division, Human Effectiveness Directorate, at Wright-Patterson Air Force Base. He received his PhD in Experimental Psychology/ Human Factors from the University of Cincinnati in 2007.

Dr. Gerald Matthews obtained his PhD in Experimental Psychology from the University of Cambridge. He joined the Institute for Simulation and Training at the University of Central Florida in 2013, having previously held a faculty position at the University of Cincinnati. His research focuses on human factors, cognitive models of personality and individual differences, and task-induced states of stress and fatigue.

Dr. Vincent Mancuso is a Postdoctoral Researcher at the U.S. Air Force Research Lab, working in the Human Performance Wing's Applied Neuroscience Branch. There he conducts research focused on cyber operator performance monitoring and optimization. He received his PhD in Information Sciences and Technology from Pennsylvania State University in 2012, and his BS in Information Systems and Human-Computer Interaction at Carnegie Mellon University in 2007.

Dr. Matthew Funke is a Research Psychologist with the Naval Medical Research Unit in Dayton, OH. He obtained his PhD in Experimental Psychology/Human Factors from the University of Cincinnati in 2011.

Dr. Joel S. Warm joined the faculty of the University of Cincinnati shortly after receiving his doctorate in Experimental Psychology from the University of Alabama in 1966 and completing post-doctoral training in Human Factors at the University of Louisville. Currently, he is Professor Emeritus of Psychology at the University of Cincinnati, Senior Scientist at the Warfighter Interface Division, Human Effectiveness Directorate, Air Force Research Laboratory, Wright-Patterson AFB, OH, and Distinguished Researcher in the Human Factors Group of the University of Dayton Research Institute. Professor Warm is a Fellow of the American Association for the Advancement of Science, the American Psychological Association, the Association for Psychological Science, and the Human Factors and Ergonomics Society. He has served on two National Research Council committees, is an Associate Editor of Human Factors, *and is a member of the editorial board of* Theoretical Issues in Ergonomic Science.

Dr. Peter A. Hancock is Pegasus Professor, University Trustee Chair, and Provost Distinguished Research Professor in the Department of Psychology and the Institute for Simulation and Training at the University of Central Florida. He is a Fellow and a past President of the Human Factors and Ergonomics Society. He is a Fellow of the American Association for the Advancement of Science (AAAS), the American Psychological Association (APA), the American Psychological Society (APS), and the Royal Aeronautical Society (RAeS). His work concerns the assessment of human performance under extremes of stress. He is an acknowledged world leader in the areas of vigilance and sustained attention. He has also conducted extensive work on the human perception of time.